Submit the completed PIA to
Privacy's SharePoint Customer Center

DIS PIA

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of system: Document Imaging System

(b) Bureau: CGFS

(c) System acronym: DIS

(d) iMatrix Asset ID Number: 871

(e) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The current ATO will expire on October 31, 2016; however documentation has been submitted and accepted for reauthorization.

(c) Describe the purpose of the system:
DIS converts paper records to electronic files by scanning new submissions as well as existing paper files for current and retired Department of State (DoS) employees, their beneficiaries, and contractors. The system also accepts electronic files (email, forms, documents, etc.) that in the past would be printed out for filing. This system does not collect data directly nor is it a system of record, but provides electronic filing and storage for data collected for CGFS compensation or financial transaction service activities. This electronic filing enables account managers and technicians to accomplish their tasks

faster and without the requirement to move paper files back and forth from physical storage.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The source of information is completed forms, correspondence and other documents that are generated by DOS employees, retirees, their beneficiaries and contractors that are then scanned or imported into DIS. Documents maintained in DIS include documents that collect information on employment, retirement pay, general accounting, vendor transactions, accounts receivable, cashiering and other compensation and financial management services. Personally identifiable information (PII) that may be maintained includes names, address, social security numbers, tax identification numbers, date of birth, age, marital status, vendor information, financial banking information, beneficiary, and insurance information. The system provides storage for these documents, replacing the filing cabinets once used to house the information collected for the compensation and financial services provided by CGFS.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

Varies by client office collecting the data:

General:

22 U.S.C. 2651a (Organization of the Department of State);
22 U.S.C. 3921 (Management of Service);
5 U.S.C. 301 (Management of the Department of State);
31 U.S.C. 901-903 (Agency Chief Financial Officer's Act).

Compensation Data:

22 U.S.C. 4042 (Maintenance of the Foreign Service Retirement and Disability Fund);
42 U.S.C. 653 (the Personal Responsibility and Work Opportunity Reconciliation Act of 1996);
Executive Order 11491, as amended (Labor-management Relations in the Federal Service);
5 U.S.C. 5501-5584 (Pay Administration).

Financial Management (Accounting, Disbursing, Claims) Data:

The Federal Financial Management Act (FFMIA) of 1996.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- SORN Name and Number: Compensation - STATE-30: Personnel Payroll Records; Financial Management: State-73, Global Financial Management System
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): July 15, 2008

Dependent on the client office, data may only be or may also be searchable by Employee/Vendor Name, date range, or Employee ID.

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☐Yes ☒No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-05-xxx-xx (from the Department of State Records Disposition Schedules. The entire 05 series is dedicated to the CGFS bureau records. The DIS system may contain imaged documents from any record type described in this series.)
- Length of time the information is retained in the system: At least as indicated in the Department of State Records Disposition schedule which varies depending on the specific information types used by the client office. The retention periods for records maintained in DIS vary from 3 to 99 years, depending upon the specific type of record.
- Type of information retained in the system:
  Compensation and Financial Management information.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.
☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other - Annuitants

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No

- If yes, under what authorization?
Varies by client office (e.g. compensation) and their collection requirements. Members of the Public information is limited to vendors and individuals who have incurred debt to the Department of State. The majority of the information is U.S. Government Employees/Contractor Employees. Authorization as noted under response to 3(e) and 3(f).

(c) How is the information collected?

Via completed electronic or paper forms. The specific information collected varies by client office.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

The data is reviewed by client office personnel when the information is originally submitted on paper forms. The accuracy of the information is dependent on the quality controls established by each client office when forms are processed. DIS maintains the scanned data as an image file of the original form, ensuring accuracy of the form data as it was scanned into DIS.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The system is an electronic document storage system. Information is as current as the documents scanned into the system. Information in the forms cannot be updated once in the system; however, new forms associated with the employee, vendor or customer can be added to the logical folder containing like forms.

(g) Does the system use information from commercial sources? Is the information publicly available?

No

(h) Is notice provided to the individual prior to the collection of his or her information?

Each client office is responsible for providing notice to individuals to whom they are providing service concerning the collection of data associated with the forms eventually scanned into the DIS system. The DIS system itself does not directly collect information.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☒No

- If yes, how do individuals grant consent?

Not applicable to the DIS system. As noted in 4(h), DIS does not collect information directly, it only stores completed forms and documents. Each client office is responsible for ensuring that their customers have been provided the opportunity to grant consent.

- If no, why are individuals not allowed to provide consent?

Not applicable to the DIS system. As noted in 4(h), DIS does not collect information directly, it only stores completed forms and documents. Each client office is responsible for ensuring that their customers have been provided the opportunity to decline provision of information.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
Each client office understands that they are required to meet all privacy requirements and concerns for information that they collect which is then scanned or imported into DIS for storage.

5. Use of information

(a) What is/are the intended use(s) for the information?
Specific information and use varies by client office, but overall DIS provides storage and retrieval functions for a client office's business documents related to the services provided, replacing physical paper filing.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes.

(c) Does the system analyze the information stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the information?
The only analysis done on scanned forms/documents is manual indexing of key fields for retrieval purposes. Each client office defines their key fields and populates/verifies the indexing when documents are scanned.

(2) Does the analysis result in new information?
No, key fields contain data derived from the forms/documents submitted.

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☒No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
From the DIS system, PII and other data categorized as Moderate information is only available to the client office that scanned the document in via security roles in place for the application.

(b) What information will be shared?
Information is not shared from the DIS system with those outside of the client offices scanning the data into DIS.

What is the purpose for sharing the information?
Information is not shared from the DIS system with those outside of the client offices scanning the data into DIS.

(c) The information to be shared is transmitted or disclosed by what methods?

Information is not shared from the DIS system with those outside of the client offices scanning the data into DIS.

(d) What safeguards are in place for each internal or external sharing arrangement?
Information is not shared from the DIS system with those outside of the client offices scanning the data into DIS.

(e) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
Information is not shared from the DIS system with those outside of the client offices scanning the data into DIS.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
DIS does not collect data directly and access gained to information stored in DIS would be through the respective client office. Each client office that collects data for storage in DIS has procedures in place for allowing individuals to request and obtain access to the information that client office collects.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☒No

If yes, explain the procedures.
DIS is not a system of record, but an electronic filing system. If an individual wished to correct inaccurate or erroneous information, they would request that update in the system of record for the information through the client office. Thus, the individual would get his or her information corrected, but this would only be reflected in the DIS system by the scanning of additional forms or correspondence providing artefacts of the processing of that correction in the system of record.

If no, explain why not.
The form(s) by which such a correction might be requested to fix the issue within a system of record might be scanned into DIS as part of a folder for that individual or transaction, but there would be nothing in DIS to "correct" directly.

(c) By what means are individuals notified of the procedures to correct their information?
This is a client office function and is dependent on the types of information they are collecting.

8. Security Controls

(a) How is the information in the system secured?
All system configurations are done per Bureau of Diplomatic Security's (DS) Security Guidelines where they exist (e.g., Windows Server, IIS, Oracle) and the other custom components are configured per vendor best practices for security. Access to the backend

(i.e., server, database) is restricted to the Office of Global Systems Operations (CGFS/GSO) systems staff, and Windows/Active Directory (AD) accounts and groups are used to limit access to the operating system, system files and application/database files. Access to user management controls is restricted to the CGFS Information Systems Security Office (ISSO.)

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Internal access to DIS is limited to authorized staff with a need to access the system in the performance of their official duties. All users maintain at least a Public Trust security clearance level in order to gain access to the Department's unclassified computer network. To access the electronic records maintained, the individual must first be an authorized user of the Department's unclassified computer network. Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed in order for the individual to perform his or her official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). To access DIS specifically, a user must have access approved by a supervisor and provisioned by the CGFS ISSO. The system uses Single Sign-On, so no new DIS specific account is provided – the user's AD account is provided provisioned with access to the DIS system. Users are required to have a need to see the information before being granted access. Each client office has its own DIS instance with separate database and secure electronic storage location. Within each client instance, role-based security is implemented to further distinguish least privilege and to ensure need to know requirements are maintained.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Completed applications are reviewed and approved by the Information System Security Officer (ISSO) prior to assigning the individual a logon. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity (expected and unexpected) is monitored, logged and audited at the operating system/file, database and application levels by the ISSO. Detection of any unexplained activity would trigger an Incident Response action. Annual audits are done to review user accounts and access levels.

(d) Explain the privacy training provided to authorized users of the system.

All users are required to undergo computer security and privacy awareness training prior to being given access to the system and must complete refresher training yearly in order to retain access.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☐Yes ☒No
If yes, please explain.
Testing is currently underway for the encryption of the Oracle databases using Oracle's implementation of Transparent Data Encryption (TDE) at the file level. This is expected to be implemented within the next few months and should be in place for the recertification A&A of DIS in the next few months.

(f) How were the security measures above influenced by the type of information collected?
Given that the system was categorized as a Moderate system, the appropriate National Institute of Standards and Technology (NIST) 800-53 security controls were selected. The security measures above are a result of implementing said security controls.

9. Data Access

(a) Who has access to data in the system?
CGFS bureau staff in each client office has access to data scanned into DIS by the client office.

(b) How is access to data in the system determined?
The director of each client office determines what roles will be utilized for that client office. Staff within each client office can submit access requests to the CGFS ISSO to gain access. Such requests must be accompanied by the review and approval of their supervisor. The CGFS ISSO then provisions access to the client instance with the requested role(s) using the requestor's AD user account.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
Users only have access to data for their own client office. This is due to each office having a distinct physical database and data storage location. Within each client office instance, additional access restrictions are applied based on assigned roles for that user.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?
The distinct client office instances and role-based access controls described above prevent users from having access to data other than that which they have a business need to see and work with.